Strengthening Computer Network Protection Laws

Jeremy Storer outlines proposals to amend interception legislation and the implications for computer network owners and operators.

In July 2009, the Australian Government released a discussion paper calling for public submissions on proposals set out in exposure draft legislation to amend the *Telecommunications (Interception and Access) Act 1979* (Cth) (**Interception and Access Act**) to assist Australians to protect their computer networks from malicious attack and other inappropriate activities.

Currently, interception legislation in Australia only allows national security and law enforcement agencies to protect their networks appropriately – these provisions are due to expire on 13 December 2009.

the Australian Government is seeking to amend the Interception and Access Act to clarify the circumstances in which intercepting, accessing and using communications that pass over a computer network is permissible

For other members of the community, the legislation does not currently provide sufficiently clear guidance on when network activity can be lawfully monitored.. Furthermore, there is little guidance on the legitimate use and disclosure of information accessed by network owners and operators for network protection purposes. Such arrangements, as they currently stand, may expose network owners and operators to inadvertent breaches of the law when monitoring their networks for potentially harmful attack and inappropriate use of computer systems by employees and other users. This could also have the effect of rendering such information inadmissible as evidence in disciplinary processes or criminal prosecutions.

Consequently, the Australian Government is seeking to amend the Interception and Access Act to clarify the circumstances in which intercepting, accessing and using communications that pass over a computer network is permissible.

Network protection

Under the proposed approach, a new s 7(2)(aa) of the Interception and Access Act will provide that accessing communications passing over a computer network without the knowledge of the sender will not constitute unlawful interception if:

- the interception is carried out by a person appointed in writing to carry out duties relating to the protection, operation or maintenance of the network or ensuring its appropriate use; and
- the interception is reasonable necessary for the performance of those duties.

A person will also be permitted under new ss 63(C) and 63(D) of the Act to use and disclose lawfully intercepted communications if it is reasonably necessary to do so for the purpose of protecting the network, or to respond to an inappropriate use of the network.

The person responsible for the computer network must ensure that intercepted communications and other such records are destroyed if no longer required for any of the above legitimate purposes contemplated by the Act. The proposed amendments will not authorise interception of speech for network protection purposes.

Appropriate use of a computer network

The proposed amendments in s 6AAA of the Act will also enable network owners and operators to ensure that their networks are used appropriately by obtaining written undertakings from their employees to use the network in accordance with any reasonable conditions specified by the owner or operator. Where such an undertaking has been given, the network owner or operator will be entitled to use or disclose information collected about inappropriate use by employees for disciplinary purposes.

However, such information can only be disclosed for disciplinary purposes where no other Commonwealth, State or Territory law would prohibit such use or disclosure. This ensures that employers cannot circumvent existing workplace relations requirements by accessing information under the Interception and Access Act.

If a written undertaking has not been given, then intercepted communications cannot be used or disclosed to relevant authorities for disciplinary or other related purposes.

Legislation is expected to be introduced to the parliament and passed by December 2009, prior to expiry of the current laws.

In anticipation of changes to the law, network owners and operators should review their processes and ensure that they have appropriate IT user agreements in place with all of their employees, so that they are able to monitor their computer systems effectively for network protection purposes.

Legislation is expected to be introduced to the parliament and passed by December 2009

In order to be effective, such user agreements will need to be in writing, and their terms must be reasonable in all the circumstances.

The draft legislation does not prescribe what will constitute reasonable or appropriate use, recognising that circumstances may vary, depending on the nature and size of the network owner's organisation, the role of its employees and the duties they may be required to undertake.

However, reasonable terms of use will generally include matters such as permitting moderate use of electronic resources for personal reasons subject to material impact on network performance for legitimate business requirements, prohibiting access to client records other than for work-related purposes, avoiding intentional interference with network capacity, taking steps to prevent virus downloads or other malware, compliance with copyright, privacy and spam laws, and not using electronic resources to download offensive or unlawful material.

Jeremy Storer is a Senior Associate at Blake Dawson in Sydney.